

GLITSS POLICY BRIEF

Turning GLITSS Insights into Policy Impact

Closing the Gap Between Artificial Intelligence (AI), the Law, and Illicit Trade

DOI:10.5281/zenodo.20527717

Noemia Bessa Vilela, Maria Curie-Skłodowska University in Lublin, Andrius Puksas, Vytautas Magnus University, Karol Bieńkowski, Institute of Law Studies, Polish Academy of Sciences

Key Messages

- **Artificial Intelligence (AI) is advancing faster than legal systems can adapt**, creating regulatory gaps that are increasingly exploited in illicit trade.
- The main challenges are **the speed of technological change, fragmented legal frameworks across jurisdictions, and unclear liability** when AI-enabled harms occur.
- Criminal networks **benefit from cross-border operations that outpace traditional law enforcement and legal cooperation mechanisms**.
- Effective policy should focus on **harmful conduct rather than specific technologies** and should strengthen **accountability, cooperation, and enforcement capacity**.

Context & Purpose

AI has become cheap, capable, and everywhere, and the legal systems meant to govern it cannot **keep up**. The mismatch is sharpest in illicit trade, where criminals exploit fast technology, fragmented rules, and blurred responsibility all at once. Waiting for a perfect rulebook quietly favours the people already working the gap. This brief sets out why the law keeps losing ground and what would help. It is intended for lawmakers, regulators, and enforcement leaders and seeks **to explain why current legal frameworks struggle to address AI-enabled illicit trade** while proposing practical policy responses.

Insights & Findings

The growing gap between the pace of AI development and the speed of legal adaptation has created significant governance challenges, particularly in the context of illicit **trade**. **Three interconnected factors drive this problem: the inability of legislation to keep pace with technological change, the fragmentation of AI regulation across jurisdictions, and the uncertainty surrounding liability for AI-enabled harms**. These challenges are further compounded by the transnational nature of illicit activities, which frequently span multiple countries and exploit differences between legal **systems**. At the same time, we would like to highlight that overly restrictive regulation may weaken the use of AI by law enforcement, financial institutions, and digital platforms for the detection and prevention of criminal activity.

Policy Relevance

Our brief contributes to ongoing debate on AI governance by emphasizing **the need for adaptive and outcome-oriented regulatory approaches**. Our brief is particularly relevant for policymakers concerned with illicit trade, fraud, digital impersonation, and cross-border enforcement. Rather than focusing on the technology itself, we argue that **effective governance should target harmful conduct, establish clear lines of accountability, and strengthen international cooperation**. In doing so, the brief provides a practical framework for balancing innovation, security, and enforcement in an increasingly AI-driven environment.



Source: ChatGPT, prompt: „[AI vs Law]“, OpenAI, generated June 3, 2026

Recommendations

- **Regulate conduct, not the technology**. Target fraud, deception, and harm rather than freezing technical definitions the next model will outgrow. Rules built around outcomes age far better than rules built around a snapshot of the tech.
- **Assign liability along the whole chain**. Make responsibility clear among developers, deployers, platforms, and resellers, and pair it with safe harbours for parties acting in good faith, so the people building defences are not punished for taking part.
- **Create legal categories that fit**. Build clear offenses for synthetic media fraud and digital impersonation, since existing trademark, fraud, and identity laws were never written for content a machine produces on demand.
- **Invest in cooperation across borders**. Speed up the sharing of evidence, fund joint task forces, and harmonize core definitions so criminals can no longer profit from the seams between national systems.
- **Equip and protect the defenders**. Resource enforcement to actually use AI tools, and steer clear of rules that would chill the detection systems banks, platforms, and investigators rely on every day.
- **Reach the enablers**. Extend accountability to the platforms, payment processors, and infrastructure that make abuse possible at scale, an approach several jurisdictions are already starting to test.
- **Reduce fragmentation at home**. Conflicting internal rules, such as clashing national and state laws, are a vulnerability in their own right. Coherence is a security measure, not just an administrative nicety.

The law will never be quick enough to lead AI, and it does not need to be. **The realistic aim is to be limber enough to stop standing still while the illicit economy sprints ahead**. None of these steps closes the gap overnight, but together they move the law from chasing the technology to shaping the conduct around it.

Contact & Attribution

Noemia Bessa Vilela, Maria Curie-Skłodowska University in Lublin, noemia.bessavilela@mail.umcs.pl

Andrius Puksas, Vytautas Magnus University, andrius.puksas@vdu.lt

Karol Bieńkowski, Institute of Law Studies, Polish Academy of Sciences, k.bienkowski@inp.pan.pl

You can find more information in GLITSS Trilogy, Volume 3, Chapter 7 entitled: “Human-Centric AI in Law Enforcement: Legal, Ethical, and Operational Challenges for Combating Illicit Trade”